

IN THE CLAIMS:

Please amend claims 1, 8, 9, 12, 15, 16, 19, 20, 24, 27, 31, 33, and 35 as follows.

Please cancel claims 25, 26 and 28 without prejudice or disclaimer. Please add new claims 36-41 as follows.

1. (Currently Amended) A method, comprising:

~~sending~~receiving a request for registration from a user equipment ~~to~~at a serving controller via a second controller, said request for registration including information indicative of at least one ~~security-mechanism-protocol~~protocol supported by the user equipment;

determining, based on the information, in the second controller that the user equipment supports a second ~~security-mechanism-protocol~~protocol other than a first ~~security-mechanism-protocol~~protocol;

removing the information from the request for registration in the second controller, including in the request for registration an indication that the second ~~security-mechanism-protocol~~protocol is used by the user equipment and forwarding the request for registration including said indication to the serving controller; and

sending a challenge in accordance with the second ~~security-mechanism-protocol~~protocol from the serving controller to the user equipment via the second controller.

2. (Previously Presented) A method as claimed in claim 1, further comprising:

forwarding a response to the challenge in a message from the user equipment to the serving controller.

3. (Original) A method as claimed in claim 2, further comprising:

using the response for authentication of the message at the serving controller.

4. (Previously Presented) A method as claimed in claim 1, further comprising:

receiving at the second controller comprising a network entity providing proxy call state control functions between the user equipment and the serving controller.

5. (Previously Presented) A method as claimed in claim 1, wherein the sending of the request for registration from the user equipment to the serving controller comprises

sending a challenge from the serving controller to the user equipment, sending a response to the challenge from the user equipment, and

registering the user equipment to the serving controller only if a satisfactory response is received from the user equipment, and sending a further challenge to the user equipment after the registration is completed.

6. (Original) A method as claimed in claim 1, further comprising:

obtaining data for sending the challenge from a user information database.

7. (Previously Presented) A method as claimed in claim 1, wherein the sending of the challenge comprises sending the challenge comprising an authentication vector.

8. (Currently Amended) A method as claimed in claim 1, further comprising:

providing the first ~~security mechanism~~ protocol comprising a ~~security mechanism~~ protocol in accordance with a secure internet protocol.

9. (Currently Amended) A method as claimed in claim 1, further comprising:

providing the second ~~security mechanism~~ protocol comprising a ~~security mechanism~~ protocol in accordance with a hypertext transfer digest protocol.

10. (Previously Presented) A method as claimed in claim 1, further comprising:

sending of at least the challenge or a response in a message in accordance with a session initiation protocol.

11. (Previously Presented) A method as claimed in claim 1, further comprising:

registering the user equipment with a serving controller of an internet multimedia subsystem.

12. (Currently Amended) A method as claimed in claim 2, wherein said information comprises a list of ~~security mechanisms~~ protocols supported by the user equipment, the method further comprising:

including in a security-client header of the request for registration the list of ~~security mechanisms~~ protocols supported by the user equipment;

concluding at the second controller based on the list that the user equipment supports the second ~~security mechanism~~ protocol instead of the first ~~security mechanism~~ protocol;

removing the security-client header from the request and including into an authorization header of the request the indication that the second ~~security mechanism~~ protocol is to be used; and

forwarding the request to the serving controller.

13. (Previously Presented) A method as claimed in claim 1, wherein the sending of the challenge comprises sending the challenge to the user equipment in an authentication information header of a message.

14. (Original) A method as claimed in claim 3, further comprising:

providing the message comprising a request for a service provided by an application server.

15. (Currently Amended) A system, comprising:

a serving controller configured to accept registrations of user equipments and to support at least two different ~~security mechanisms~~ protocols; and

a second controller configured to receive from a user equipment in a request for registration data indicative of at least one ~~security mechanism~~ protocol that the user equipment supports, to remove said data from the request for registration, to provide the serving controller with information regarding a ~~security mechanism~~ protocol supported by the user equipment that has requested to be registered to the serving controller, and to forward the request for registration to the serving controller, wherein the serving controller is configured to send a challenge in accordance with a determined ~~security mechanism~~ protocol to the user equipment and to authenticate a message from the user equipment based on a response to the challenge included in the message.

16. (Currently Amended) A system as claimed in claim 15,

wherein the second controller configured to provide information regarding the ~~security mechanism~~ protocol is provided in a second controller.

17. (Previously Presented) A system as claimed in claim 16, wherein the

second controller comprises a network entity providing proxy call state control functions between the user equipment and the serving controller.

18. (Previously Presented) A system as claimed in claim 15, further comprising:

a user information database configured to store data associated with challenges.

19. (Currently Amended) A system as claimed in claim 15, wherein the serving controller is configured to support a ~~security mechanism~~ protocol in accordance with a secure internet protocol.

20. (Currently Amended) A system as claimed in claim 15, wherein the serving controller is configured to support a ~~security mechanism~~ protocol in accordance with a hypertext transfer digest protocol.

21. (Previously Presented) A system as claimed in claim 15, the communication system comprising an internet multimedia subsystem.

22. (Previously Presented) A system as claimed in claim 15, further comprising:

a connection to an application server, wherein a message subjected to authentication by the servicing controller based on the response to the challenge comprises a request for a service provided by the application server.

23. (Previously Presented) A system as claimed in claim 15, wherein the message subjected to authentication by the servicing controller based on the response to the challenge comprises a request for registration to the serving controller.

24. (Currently Amended) An apparatus, comprising:

a receiver configured to receive a request for registration from a user equipment for forwarding to a serving controller, said request including data indicative of at least one ~~security mechanism~~ protocol supported by said user equipment; and

a controller configured to determine based on said data a ~~security mechanism~~ protocol supported by the user equipment that has requested to be registered to the serving controller, to remove the data from the request for registration in the second controller before forwarding said request to the serving controller, and to signal information to the serving controller regarding the ~~security mechanism~~ protocol supported by the user equipment.

Claim 25. (Canceled).

Claim 26. (Canceled).

27. (Currently Amended) An apparatus, comprising:

receiving means for receiving a request for registration from a user equipment for forwarding to a serving controller, said request including data indicative of at least one ~~security mechanism~~ protocol supported by said user equipment;

determining means for determining, based on said data, a ~~security mechanism~~ protocol supported by the user equipment that has requested to be registered to the serving controller;

removing means for removing the data ~~indicative~~ from the request for registration in the second controller before forwarding said request to the serving controller; and

signalling means for signalling information to the serving controller regarding the ~~security mechanism~~ protocol supported by the user equipment.

Claim 28. (Canceled).

29. (Previously Presented) The apparatus according to claim 24, wherein the controller is further configured to send a response to the challenge from the user equipment to the serving controller.

30. (Previously Presented) The apparatus according to claim 29, wherein the controller is further configured to use the response for authentication of the message at the serving controller.

31. (Currently Amended) The apparatus according to claim 24, wherein the ~~second controller is comprised~~ comprises ~~comprised in~~ a network entity providing proxy call state control functions between the user equipment and the serving controller.

32. (Previously Presented) The apparatus according to claim 24, wherein the controller is further configured to send a challenge from the serving controller to the user equipment, to send a response to the challenge from the user equipment, and to register the user equipment to the serving controller only if a satisfactory response is received from the user equipment, and to send a further challenge to the user equipment after the registration is completed.

33. (Currently Amended) The apparatus according to claim ~~24~~32, wherein the controller is further configured to obtain data to send the challenge from a user information database.

34. (Previously Presented) The apparatus according to claim 24, wherein the controller is further configured to send challenge including an authentication vector.

35. (Currently Amended) A computer program embodied on a computer readable medium, the computer program being configured to control a processor to perform:

~~sending~~ receiving a request for registration from a user equipment to ~~at~~ a serving controller via a second controller, said request for registration including information indicative of at least one ~~security-mechanism-protocol~~ supported by the user equipment;

determining, based on the information, in the second controller that the user equipment supports a second ~~security-mechanism-protocol~~ other than a first-~~security-mechanism protocol~~;

removing the information from the request for registration in the second controller, including in the request for registration an indication that the second ~~security-mechanism protocol~~ is used by the user equipment and forwarding the request for registration including said indication to the serving controller; and

sending a challenge in accordance with the second ~~security-mechanism-protocol~~ from the serving controller to the user equipment via the second controller.

36. (New) A method, comprising:

receiving a request for registration from a user equipment for forwarding to a serving controller, said request including data indicative of at least one protocol supported by said user equipment;

determining, based on said data, a protocol supported by the user equipment that has requested to be registered to the serving controller;

removing the data from the request for registration in the second controller before forwarding said request to the serving controller; and

signaling information to the serving controller regarding the protocol supported by the user equipment.

37. (New) The method according to claim 36, further comprising sending a response to the challenge from the user equipment to the serving controller.

38. (New) The method according to claim 37, further comprising using the response for authentication of the message at the serving controller.

39. (New) The method according to claim 36, wherein the second controller comprises a network entity providing proxy call state control functions between the user equipment and the serving controller.

40. (New) The method according to claim 36, further comprising forwarding a challenge including an authentication vector.

41. (New) A computer program embodied on a computer readable medium, the computer program being configured to control a processor to perform:

receiving a request for registration from a user equipment for forwarding to a serving controller, said request including data indicative of at least one protocol supported by said user equipment;

determining, based on said data, a protocol supported by the user equipment that has requested to be registered to the serving controller;

removing the data from the request for registration in the second controller before forwarding said request to the serving controller; and

signaling information to the serving controller regarding the protocol supported by the user equipment.